



DEPARTMENT OF THE NAVY

NAVAL SPACE COMMAND  
FALLS CHURCH VIRGINIA 22448-5170

REF ID: A66666

NAVSPACECOMINST 5530.1A  
OOI/OOM

FEB 23 1987

NAVSPACECOM INSTRUCTION 5530.1A

Subj: PHYSICAL SECURITY

Ref: (a) OPNAVINST 5530.14A  
(b) OPNAVINST 3850.4A  
(c) OPNAVINST 5510.1G  
(d) SECNAVINST 5500.4D  
(e) NAVSPACECOMINST 5400.1

Encl: (1) Threat Conditions, Countermeasures, and Assessment Factors  
(2) Activity Security Checklist, Standard Form 701  
(NSN 7540-01-213-7899)

1. Purpose. To establish policy and procedures for the physical security of the Naval Space Command (NAVSPACECOM) Headquarters and to provide guidance to subordinate commands in establishing security programs and plans. The requirements of references (a) through (d) are specifically applied herein to the following areas:

- a. Security of buildings and spaces
- b. Handling and safeguarding classified materials
- c. Access to restricted areas
- d. Keys, key lockers and key control
- e. Antiterrorism

2. Cancellation. NAVSPACECOMINST 5530.1.

3. Scope. This instruction applies to all physical security, antiterrorism, and loss prevention matters throughout NAVSPACECOM. It includes coordination and support between command and host installations. Host physical security guidelines will prevail outside the confines of NAVSPACECOM component facilities. Reference (e) contains headquarters specific procedures.

4. Discussion. All echelons within the chain of command must focus attention and direction on overall physical security, loss prevention, and antiterrorism programs. Each commanding officer will:

- emphasize the need for such programs,

FEB 23 1987

- ensure that the total security posture of the activity is thoroughly and accurately assessed, and
- ensure that security resources (including properly motivated, trained, and equipped personnel) are available to implement programs.

5. Terrorist Threat Conditions (THREATCONS). Antiterrorist measures are inherent in physical security and shall be reflected in physical security programs, plans, exercises, and operations. The definitions below apply within NAVSPACECOM.

a. Terrorism. Unlawful use or threatened use of force or violence by a revolutionary organization against individuals or property, often for political or ideological purposes, with the intention of coercing or intimidating governments or societies.

b. Antiterrorism. Defensive measures used by DOD to reduce vulnerability of DOD personnel, their dependents, facilities, and equipment to terrorist acts.

c. Counterterrorism. Offensive measures taken to respond to a terrorist act, including the gathering of information and threat analysis in support of these measures.

d. Threat Condition (THREATCON). Formal levels of antiterrorist readiness, directed by commanding officers to upgrade physical security readiness to deter terrorist acts. Enclosure (1) presents specific threat conditions and appropriate countermeasures. Area coordinators are the lead agencies in coordinating and setting/changing THREATCONS.

6. Self-Inspection Program. All commands will perform annual self-inspections/surveys and periodic checks in accordance with references (a) and (b).

a. Appendix VIII of reference (a) and Exhibit 2C of reference (c) provide annual self-inspection/survey checklists.

b. The appropriate paragraphs in references (a) and (c) provide guidance in conducting periodic spot checks including, but not limited to:

(1) Facility security checks (daily, on weekends and holidays) using enclosure (2).

(2) Materials/folders for proper marking (periodic).

(3) Messages for records of derivative classifications (periodic).

(4) Safes for dates of combination changes (periodic), etc.

7. Missing, Lost, Stolen or Recovered (MLSR) Government Property. All commands will establish programs for reporting MLSR government property to proper authority per reference (d). Tenant commands may obtain assistance from host security/criminal investigative resources when the host-tenant or other agreement provides for such services.

8. Civil Authorities. When civil authorities wish to enter NAVSPACECOM facilities, the host security officer will notify the command security officer during normal working hours or the CDO after hours. Only commanding officers may approve the release of military personnel to civil authorities.

9. Responsibilities. Security is the direct, immediate, legal, and moral responsibility of all military and civilian personnel. At no time shall classified material be left unattended or unauthorized personnel be permitted access to work spaces.

a. Echelon Three commanders are responsible for ensuring implementation of this instruction including verification of compliance by subordinate commands or detachments through a viable assistance visit/inspection program. Commanders/Commanding Officers may issue amplifying instructions which include coordination and compliance with host activity procedures.

b. Commanding Officers are responsible for physical security, loss prevention, and antiterrorism programs at their level of command. They will:

(1) Designate in writing, by name, a Security Officer.

(2) Designate in writing all restricted areas.

(3) Establish a key and lock control program (including key cards/badges) where appropriate.

(4) Develop a security plan which includes procedures for emergency destruction, bomb threats, antiterrorism, severe weather, visitor control, periodic inspections/checks, etc. Tenant activities may adopt host activity programs, as applicable, governed by compliance with the intent of this instruction and references (a) and (c).

FEB 23 1987

(5) Establish a Physical Security Review Board (PSRB), a Physical Security Review Committee (PSRC), and a Loss Prevention Subcommittee (LPS) or appoint representatives to Host command bodies.

(6) Establish procedures for self-inspections and checks.

(7) Route new construction requirements, prepared per reference (a), for review by the NAVSPACECOM Security Officer (OOM) and the Director, Logistics and Information Systems Division (N4/6).

c. COMNAVSPACECOM will chair the command Physical Security Review Board (PSRB). This board, with goals and purposes similar to those of a Physical Security Review Committee (PSRC), will meet at least annually. A specific goal of the board is coordination of supportive physical security and loss prevention practices between headquarters and subordinate commands. Permanent board members are: Commanding Officers of third echelon commands, Headquarters Security Officer, and NAVSPACECOM Inspector General. Other staff members may be called upon to participate, depending on site-sensitive activities.

d. The NAVSPACECOM Inspector General will:

(1) Review physical security, antiterrorism and loss prevention programs when inspecting subordinate commands.

(2) Conduct annual inspections/surveys and periodic spot checks of the headquarters security programs per references (a) and (c).

e. Security Officers report to the Commander/Commanding Officer via the Deputy Commander/Executive Officer. They are responsible for:

(1) Assisting and advising the commander by managing the physical security, antiterrorism, and loss prevention programs. This includes assessing the adequacy of the programs and recommending improved measures. Reference (a) describes these duties in detail.

(2) Conducting periodic personnel/visitor and parcel inspections, visually checking their appearance and looking into briefcases, purses, etc., at entry and exit points of command spaces.

(3) Starting a preliminary investigation of a Missing, Lost, Stolen, or Recovered (MLSR) report within 72 hours and notifying higher authority as required.

FEB 18 1987

(4) Providing comments to NAVPSACECOM (N4/6) per reference (a) on new construction requirements.

(5) Conducting an annual review of 10% of Personnel Security Investigations (PSIs) completed by host commands to ensure that personnel security records are current.

(6) Coordinating all aspects of the various security programs to enhance the command security posture.

F. The Director, Logistics and Information Systems Division (N4/6) is responsible for ensuring that new construction requirements comply with reference (a) and DM 13-1, NAVFAC Design Manual for Physical Security.

g. All personnel are responsible for:

(1) The security of their working area during regular hours.

(2) Assisting in enforcing the procedures in this instruction.

(3) Immediately reporting irregularities to their immediate supervisor, the Security Officer (CDO after hours), or the Inspector General.

(4) Monitoring the activities of all visitors while in their spaces.

(5) Complying with motor vehicle and traffic control rules and regulations of the host activity (where applicable).

10. Forms. At headquarters, enclosure (2) is available from N172. Subordinate commands shall order SF 701 from the Federal Supply Service using FEDSTRIP/MILSTRIP procedures.



R. C. MACKE

Distribution:

List IA

NAVSPASUR

NAVASTROGRU

FLTSURVSUPPCOM

Copy to:

NAVSWC

PACMISTESTCEN

NAVSECGRUACT NORTHWEST

THREAT CONDITIONS, COUNTERMEASURES, AND ASSESSMENT FACTORS

I. THREAT CONDITIONS AND COUNTERMEASURES

a. Threat Condition ALPHA. This condition applies when there is a general threat of possible terrorist activity against installations and personnel, the nature and extent of which are unpredictable, when the circumstances do not justify full implementation of the measures of THREATCON BRAVO. However, it may be necessary to implement certain selected measures from THREATCON BRAVO as a result of intelligence received or as a deterrent. The measures in this THREATCON must be capable of being maintained indefinitely.

(1) Measure 1. At regular intervals, remind all personnel, including dependents, to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers; alert for unidentified vehicles on, or in the vicinity of U.S. installations; alert for abandoned parcels, suitcases, or any unusual activity.

(2) Measure 2. Keep available, at all times, the duty security officer or other appointed personnel who have access to plans for evacuating buildings and areas in use and for sealing off any areas where an explosion or attack has occurred. Keep on call key personnel who may be needed to implement security plans.

(3) Measure 3. Secure buildings, rooms, and storage areas not in regular use.

(4) Measure 4. Increase security spot checks of vehicles and persons entering the installations and nonclassified areas under the jurisdiction of the U.S. command and agency.

(5) Measure 5. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

(6) Measure 6. As a deterrent, apply one of the following measures from THREATCON BRAVO individually and randomly.

(a) Secure and regularly inspect all buildings, rooms, and storage areas not in regular use. (Measure 14)

(b) At the beginning and end of each workday and at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious activity or packages. (Measure 15)

FEB 25 1987

(c) Check all deliveries to messes, clubs, etc. (Advise dependents to check all home deliveries.) (Measure 17)

(d) As far as resources allow, increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense and to build confidence among staff and dependents. (Measure 18)

(7) Measure 7. Review all plans, orders, personnel details, and logistic requirements related to the introduction of the higher THREATCON.

(8) Measure 8. Review and implement, as appropriate, security measures for high-risk personnel.

(9) Measure 9. Spare.

b. Threat Condition BRAVO. This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing undue hardship, without affecting operational capability, and without aggravating relations with local authorities.

(1) Measure 10. At regular intervals, remind all personnel including dependents, to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers; alert for unidentified vehicles on, or in the vicinity of U.S. installations; alert for abandoned parcels or suitcases or any unusual activity.

(2) Measure 11. Keep all personnel involved in implementing anti-terrorist contingency plans on call.

(3) Measure 12. Check plans for implementation of the measures contained in the next THREATCON.

(4) Measure 13. Where possible, cars and such objects as crates, trash containers, etc., are to be moved at least 25 meters from buildings, particularly those buildings of a sensitive or prestigious nature. Consider the application of centralized parking.

(5) Measure 14. Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.

(6) Measure 15. At the beginning and end of each work day and at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

FEB 23 1987

(7) Measure 16. Examine all mail for letter or parcel bombs. (This examination is increased above normal.)

(8) Measure 17. Check all deliveries to messes, clubs, etc. (Advise dependents to check all home deliveries.)

(9) Measure 18. As far as resources allow, increase surveillance of domestic accommodations, schools, messes, and clubs, to build confidence among staff and dependents.

(10) Measure 19. Make staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.

(11) Measure 20. At an early stage, inform members of local security committees of any action being taken and why.

(12) Measure 21. Upon entry of visitors to the unit, physically inspect them and a percentage of their suitcases, parcels, and other containers.

(13) Measure 22. Wherever possible, operate random patrols to check vehicles, people, and buildings.

(14) Measure 23. Protect off-base military personnel and military transport in accordance with prepared plans. Remind drivers to lock parked vehicles and to institute a positive system of checking before they enter and drive a car.

(15) Measure 24. Implement additional security measures for high-risk personnel as appropriate.

(16) Measure 25. Brief personnel who may augment guard force on use of deadly force.

(17) Measure 26-29. Spare.

c. Threat Condition CHARLIE. This condition applies when an incident occurs or when intelligence is received indicating that some form of terrorist action against installations and personnel is imminent. Implementation of this measure for more than a short period will probably create hardship and will affect the peacetime activities of the unit and its personnel.

(1) Measure 30. Continue all THREATCON BRAVO measures or introduce those outstanding.



FEB 23 1987

(2) Measure 31. Keep available at their places of duty all personnel who are responsible for implementing anti-terrorist plans.

(3) Measure 32. Limit access points to absolute minimum.

(4) Measure 33. Strictly enforce control of entry and search a percentage of vehicles.

(5) Measure 34. Enforce centralized parking of vehicles away from sensitive buildings.

(6) Measure 35. Issue weapons to guards. (Local orders should include specific orders on issue of ammunition.)

(7) Measure 36. Introduce increased patrolling of the installation.

(8) Measure 37. Protect all designated vulnerable points (VP) and give special attention to VP outside military establishments.

(9) Measure 38. Erect barriers and obstacles to control traffic flow.

(10) Measure 39. Spare.

d. Threat Condition DELTA. This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely. Normally, this THREATCON is declared as a localized warning.

(1) Measure 40. Continue or introduce all measures listed for THREATCONs BRAVO and CHARLIE.

(2) Measure 41. Augment guards as necessary.

(3) Measure 42. Identify all vehicles entering the complex or installation as well as the vehicles' contents.

(4) Measure 43. Search all vehicles entering the complex or installation as well as vehicles' content.

(5) Measure 44. Control all access and implement positive identification of all personnel.

(6) Measure 45. Search all suitcases, briefcases, packages, etc., brought into the complex or installation.

FEB 22 1987

(7) Measure 46. Take measures to control access to all areas under the jurisdiction of the U.S. command or agency.

(8) Measure 47. Make frequent checks of the exterior of concerned buildings and of parking areas.

(9) Measure 48. Minimize all administrative journeys and visits.

(10) Measure 49. Consult local authorities about closing public (and military) roads and facilities that might make sites vulnerable to terrorist attack.

(11) Measure 50. Spare.

## 2. ASSESSMENT FACTORS FOR UNIFORM IMPLEMENTATION OF SECURITY ALERT CONDITIONS

a. Existence. Applies when a terrorist group is present in an area of concern. Group need not have posed a threat to U.S. or DOD interest in the past.

b. Capability. Applies when a terrorist group has the ability to carry out an operation against U.S. interests in areas of concern. This includes resources such as intelligence, mobility, personnel, etc.

c. History. Applies when a group's history of terrorist acts and behavior reflect an anti-U.S. stand or includes previous attacks against U.S. interests.

d. Trends. Applies if the group has, over the past year, displayed significant terrorist activity that appears to be continuing or increasing. Activity need not have been violent; i.e., terrorist attack against U.S. or DOD interest could be rhetorical or threatening utterances or statements. This factor could be flexible depending on the length of the group's activity cycle.

e. Targeting. Applies if there are known plans or confirmed intentions of a terrorist group to target U.S. or DOD interests. Targeting can be either specific or non-specific. If targeting is not against U.S. or DOD interest, this factor should not be considered.

ACTIVITY SECURITY CHECKLIST	DIVISION/BRANCH/OFFICE	ROOM NUMBER	MONTH AND YEAR
-----------------------------	------------------------	-------------	----------------

Irregularities discovered will be promptly reported to the designated Security Office for corrective action.

Statement

I have conducted a security inspection of this work area and checked all the items listed below.

I have conducted a security inspection of this work area and checked all the items listed below.

TO (If required)

FROM (If required)

THROUGH (If required)

SAMPLE

FEB 23 1987

701-101  
NSN 7540-01-213-7899

U.S. GOVERNMENT PRINTING OFFICE: 1985-461-275/20198

STANDARD FORM 701 (8-85)  
Prescribed by GSA/ISO  
32 CFR 2003

Enclosure (2)